Testimony in support of SB 195 - The Montana Electronic Privacy Act

Testimony submitted on behalf of University of Montana law students and drafters of SB 195: John C. Bacino, Nicholas J. Hyde, Bradley R. Jones & Keif A. Storrar.

In 2009, the city of Bozeman gained national media attention by requiring job applicants to hand over personal passwords to all websites to supplement the City's background checks. Though Bozeman ultimately stopped the practice, there is no law preventing other employers from engaging in similar practices. Not only does this kind of practice run afoul of individuals' privacy expectations, it allows an employer to search for information it would otherwise be prohibited to ask about, such as religious beliefs, marital status, and personal communications through email. This type of behavior is akin to an employer requesting access to one's private mail, bank statements, or desk drawers as a condition of hiring or continued employment.

This bill makes it illegal for any employer to require an employee or job applicant to disclose their personal online or offline account information as a condition of employment or continued employment. It would also prohibit employers from requiring current employees to reveal their online account information, and would prohibit employers from firing or punishing employees who refuse.

This bill does not prohibit employers from searching for otherwise publicly available information either online or offline. This bill does not prevent employers from conducting due diligence investigations or background checks into their employees, nor does it prevent employers from creating their own limitations on workplace internet use. Employers retain control over their own proprietary online and offline information accessed through their own electronic devices. This bill does not prohibit law enforcement officers from conducting investigations into illegal activity in order to ensure compliance with applicable laws. Such investigations are valid when supported by either a warrant or by court order. By clarifying that employers cannot require this information, the law will absolve from liability for failing to use protected, private information to screen applicants and employees.

Six other states have passed similar laws and most recently, in late December, 2012, Michigan's governor Republican Rick Snyder signed into law a similar online privacy bill which was passed by a Republican-controlled legislature. Michigan's law is the first in the nation to establish criminal and civil penalties. This bill does not have penalties, but if the committee wished to amend the bill to include such penalties we believe this would further strengthen the bill.

Short Bill Summary:

This Act prevents public and private employers from requiring job applicants or employees to disclose access to their private personal accounts used either online or offline, or other private personal information stored either online or offline on electronic communication devices. This Act in no way prevents an employer from requiring an employee to disclose information stored either online or offline that is used in conjunction with the work being performed on behalf of the business, organization, or public agency. However, the disclosure of information related to the business activities does not extend to a personal account that is being used to promote the business activity (i.e. a Facebook event that is shared between friends who promotes the business, organization or public agency where the employee is employed). This Act in no way prevents an employer from performing online searches of the applicant or employee and accessing information that would otherwise be public. This Act is not intended to impede or prohibit law enforcement officers from conducting investigations into illegal activity in order to ensure compliance with applicable laws. Such investigations are valid when supported by: a warrant or by court order. By passing this Act the legislature would be protecting employers from any liability for failing to use protected, private information to screen applicants and employees. This Act does not repeal or modify any existing section of the Montana code.

A Montana Story

In 2009 the City of Bozeman made nationwide headlines when it was disclosed that the City required job applicants to list usernames and passwords for their social-networking sites.[1] The relevant language in the application required the applicant to sign a waiver disclosing:

> "any and all, current personal or business Web sites, Web pages or memberships on any Internet-based chat rooms, social clubs or forums, to include, but not limited to: Facebook, Google, Yahoo, YouTube.com, MySpace, etc."[2]

The City had required such a disclosure for years and justified the disclosure as part of their routine background checks.[3] The day after the national headlines broke, the City suspended its policy conceding that requesting such information "exceeded that which is acceptable to our community."[4] Following a formal investigation by the City Commission, the City disciplined its City Manager and three other employees for their "severe breach of public trust."[5]

The Montana Electronic Privacy Act:
A reasonable approach to a growing problem

Protecting an individual's right to online privacy is a growing concern nationwide due to the increased ease that technology allows us to broadcast our lives in cyberspace in both public and private ways. There are rising concerns that an employer could require an employee or job applicant to disclose such information as a condition of employment. With this realization, a growing number of states are taking action to protect employers and employees from any invasion of privacy in online accounts.[6]

The logical outgrowth from Montana Constitutional Rights and existing statutes

"The right of individual privacy is essential to the well-being of a free society and shall not be infringed without the showing of a compelling state interest."

—Mont. Const. art. II, § 10.

The Montana Right to Privacy Act is a logical outgrowth of the existing statutes and fundamental rights under the Montana Constitution. Both online and offline personal accounts can contain private information relating to the person's race, color, sex, culture, social origin or condition, political or religious ideas, or otherwise private comments or communications that could cause undue prejudice by the employer toward the person. Examples of personal accounts may include:

- personal online banking accounts;
- email accounts;
- online password banks that hold all personal passwords;
- social media websites (i.e. Facebook, MySpace, eHarmony, etc.);
- cloud storage accounts; and
- offline accounts associated with any and all data stored on ipads, and iphones etc., which store vast amounts of personal data in an offline setting.

Certainly, some, but not all, of the information stored on these accounts is publically accessible. Nothing in this Act prevents an employer's in screening an employee or job applicant to find publically accessible information. However, it is entirely a different situation for an employee to require disclosure of otherwise private personal account information as a condition of employment. This would be akin to an employer digging through your mailbox or personal desk drawers at home to read personal mail and documents as a condition of employment or continued employment. Such acts by an employer would be exposing personal private information that is protected under the individual's constitutional right to privacy.[7] Additionally, exposing an employer to such personal information could result in other forms of discrimination or prejudice

toward the employee or applicant that would otherwise not exist infringing upon the individual's constitutional right to dignity.[8]

The Montana Right to Privacy Act is similar to an existing Montana law prohibiting the use of a lie-detector test (polygraph) as a condition of employment or continued employment. Following the enactment of Montana's Constitution in 1972, the Legislature passed Montana Code Annotated § 39-2-304 which prohibits "A person, firm, corporation, or other business entity or its representative [from requiring] a person to take a polygraph test or any form of a mechanical lie detector test as a condition for employment or continuation of employment." The passage of this law was an outgrowth from Delegate Proposal Number 124 from the Constitutional Convention, titled: "A proposal for a new Constitutional section prohibiting lie-detector tests as a condition of employment." It was thought that the complementary protection of the right to privacy in this proposal "would offer protection against privacy invasions made as a condition of employment."[9] Although this proposal was rejected during the convention, it was in part because of the concern that it made the right to privacy too specific. In response, the legislature to passed § 39-2-304 in 1974.

The debates of the delegates to the Montana Constitutional Convention acknowledged the paramount importance of citizen's privacy and enshrined respect for privacy in some of the most protective provisions found in any constitution. The official voter pamphlet explained privacy as a "[n]ew provision prohibiting any invasion of privacy unless the good of the state makes it necessary."[10] Delegate Campbell's succinct summary of Montana's right to privacy rings like the preamble to this Act: "The basis of the right to privacy is the right to be let alone."[11] The codification of this Act has similar goals to § 39-2-304. By codifying this Act the legislature is strengthening Montanans' rights by mirroring the idea set forth in the original Constitutional debates and updating § 39-2-304 to the digital age.

Relevant Case Law

Requiring a police officer to take a polygraph test as a condition of employment was found to be unconstitutional by the Montana Supreme Court. In *Oberg v. City of Billings*, the Billings Police Commission found Oberg guilty of in insubordination when he refused a direct order to take a polygraph examination.[12] Oberg was under investigation by the Department after an arrestee filed a complaint alleging that Oberg struck him after he was detained and in handcuffs. During the investigation Oberg was ordered to submit to a polygraph examination, pursuant to § 39-2-304(2), which exempted public law enforcement agencies from compliance with the law. Oberg refused to submit to the polygraph and the Chief of Police filed charges against Oberg. The Billings Police commission ruled that Oberg's failure to comply with the order constituted insubordination. Oberg was disciplined with a six month probationary period and suspended without pay for 15 days. The City argued that because police officers "occupy a particularly high

position of public trust [] it is the goal of the City to maintain law enforcement agencies of the highest integrity."

The Montana Supreme Court acknowledged that "police officers occupy a position of public trust in our society," but held that the statute could not withstand rational basis and was an unconstitutional violation of public law enforcement agency employees' right to equal protection of laws.[13] The court reasoned that since section (2) of the statue exempted all public law enforcement agencies from the law it was overly broad because "secretaries, clerks, dispatchers, meter maids and dogcatchers" are all "employees of public law enforcement agencies as are police officers, but they do not occupy the same position of power and concomitant trust that must reside in our police forces."[14] The statute has since been amended to remove section (2) that exempted public law enforcement agencies from compliance.

The enactment of the Montana Electronic Privacy Act does nothing more than codify existing fundamental rights under the Montana Constitution. Article II, § 4 (the Right to Human Dignity) states:

> "The dignity of the human being is inviolable. No person shall be denied the equal protection of the laws. Neither the state nor any person, firm, corporation, or institution shall discriminate against any person in the exercise of his civil or political rights on account of race, color, sex, culture, social origin or condition, or political or religious ideas."

Additionally, Article II, § 10 (the Right to Privacy) states:

> "The right of individual privacy is essential to the well-being of a free society and shall not be infringed without the showing of a compelling state interest."

While the Court in *Oberg* did not reach its conclusion under strict scrutiny analysis by implicating the fundamental right to privacy, the Court noted that if "a statutory exception were enacted to specifically exclude police officers from the general statutory protection granted all other employees in this state, we doubt that such an exception would survive a sustained attack under the strict scrutiny test."[15]

Summary and Comparison of Enacted Online Privacy Legislation

Six states have each passed their own version of an online privacy bill. Most of these bills focus on prohibiting employers from asking employees and job applicants for access to online accounts, while some focus on prohibiting schools from requiring this information of students.

Michigan (Enrolled December 28, 2012 - H.B. 5523)

The Michigan law bars businesses and educational institutions, in most circumstances, from asking employees, job applicants, students and prospective students for information or passwords used to access private internet account information. The law penalizes an employer with a misdemeanor punishable with a maximum fine of $1,000 and allows for the victim to bring a civil action and recover up to $1,000 in damages plus attorneys' fees for firing, refusing to hire, or refusing admission to student because of the persons refusal to disclose such information. On Sponsor Aric Nesbitt (R) said that "an employer's request for a job applicant's Facebook password is 'the same as asking for an individual's P.O. box key and rummaging through their mail, or going through their living room to look at their personal picture albums.'"[16] Sites such as Facebook and Twitter have privacy settings for users to restrict who can see their postings, he observed. "[W]e should respect those limits that people set," he said.[17]

Maryland (MD LABOR & EMPLY § 3-712)

Maryland's statute focuses on protecting the usernames and passwords of employees and job applicants. It prohibits employers from firing or punishing employees and from refusing to hire applicants who do not give up their account information. The statute also makes clear that it does not prohibit employers from investigating employees whom the employer suspects may be sharing proprietary information.

Perhaps the strongest feature of the bill is its broad definition of an "electronic communications device." Rather than limiting itself specifically to computers, phones, and PDA's, the statute includes, "any device that uses electronic signals to create, transmit, and receive information."

Delaware (Del. Code Ann. tit. 14, § 9401-9405)

Delaware's "Education Privacy Act," as the name suggests, deals with academic institutions and students. Unlike the broader protection of the Maryland statute, it focuses on social media accounts, such as Facebook and MySpace. In addition to prohibiting institutions from requesting user names and passwords, it also prohibits institutions from requiring students to add the institution to his or her list of social network contacts.

Essentially, the Delaware Act serves the same function as any of the other online privacy statutes, but only as to educational institutions. Unfortunately, the Act also includes relatively narrow definitions and only covers social media accounts, leaving other areas of online privacy unaddressed.

California (CA LABOR § 980)

California created a short and simple statute, prohibiting employers from requesting employees' social media usernames and password, requesting access to these accounts in front of the employer, or requesting that employees divulge information from these accounts. Though California uses the term "social media," the definition has a broader scope than Delaware's statute, including just about any online account that can be used to share information. The statute also includes the standard exceptions allowing an employer to access information necessary to investigate its employees.

Illinois (IL ST CH 820 § 55/10)

The Illinois Statute is similar to Delaware's statute in that it only protects actual social media accounts, not online accounts generally, and specifically excludes e-mail. The statute also makes exceptions for employers who monitor their employees' activity on work computers. This means that an employer cannot ask for account information, but may record information if the employee accesses an account at work. Of all the enacted online privacy statutes, Illinois offers the least employee protection.

Questions and Responses to this Act:

1. **Does this bill restrict the right of employers to access publicly available information about an employee or job applicant which is not password-protected?**
   NO. This bill will not affect an employer's right to access any online information which is publically available, or not password-protected.

2. **Does this bill restrict the right of law enforcement to investigate alleged criminal activity which is password protected?**
   NO. The right of law enforcement is in no way impaired to conduct criminal investigations permitted by a court order under state or federal law.

3. **Does this Act limit employer liability for failure to use protected, private information to screen employees or job applicants?**
   YES. This Act will protect employers from liability for failing to use the protected, private information covered by this bill to screen applicants and employees. By clarifying that employers cannot require this private information, employers, by the same token, cannot be held liable for negligently hiring an employee based on this private information.

4. **Does this require a fiscal note?**
   The bill requires no appropriation by the Legislature and should have no "effect on the revenues, expenditures, or fiscal liability of the state or of a county."

[1] Amanda Ricker, *City requires Facebook passwords from job applicants*, Bozeman Daily Chronicle (June 18, 2009).
[2] Amanda Ricker, *City requires Facebook passwords from job applicants*, Bozeman Daily Chronicle (June 18, 2009).
[3] Amanda Ricker, *City requires Facebook passwords from job applicants*, Bozeman Daily Chronicle (June 18, 2009).
[4] City's suspends controversial Facebook policy, Bozeman Daily Chronicle (June 18, 2009).
[5] Amanda Ricker, *Three put on probation for hiring policy*, Bozeman Daily Chronicle (Oct. 13, 2009).
[6] California (A.B. 1844 codified in Chapter 618), Maryland (H.B. 964 / S.B. 433 codified in Chapters 232 and 234), and Illinois (H.B. 3782, Public Act 97-0875), enacted legislation in 2012 and 14 other states introduced legislation prohibiting an employer from requesting or requiring a job applicant or employee to disclose their user name(s), password(s), or other ways of accessing their personal online accounts. (*See* http://www.ncsl.org/issues-research/telecom/employer-access-to-social-media-passwords.aspx).
[7] *See* Mont. Const. art. II, § 4.
[8] *See* Mont. Const. art. II, § 4.
[9] *Id.* at 641.
[10] *Proposed 1972 Constitution* at 6 ("Right of Privacy").
[11] Mont. Const. Conv., Vol. III, 1851.
[12] *Oberg v. City of Billings*, 674 P.2d 494 (Mont. 1983).
[13] *Oberg v. City of Billings*, 674 P.2d 494, 497 (Mont. 1983).
[14] *Oberg v. City of Billings*, 674 P.2d 494, 497 (Mont. 1983).
[15] *Oberg v. City of Billings*, 674 P.2d 494, 497-498 (Mont. 1983).
[16] U.S. Law Week, Vol. 81, No. 25, 981-982, Jan. 08, 2013.
[17] U.S. Law Week, Vol. 81, No. 25, 981-982, Jan. 08, 2013.